Autenticación y autorización mediante WebAuthn MFA

ONTAP 9

NetApp
December 20, 2024

Tabla de contenidos

Autenticación y autorización mediante WebAuthn MFA

Descripción general de la autenticación multifactor de WebAuthn

A partir de ONTAP 9.16,1, los administradores pueden habilitar la autenticación multifactor (MFA) de WebAuthn para los usuarios que inician sesión en System Manager. Esto permite los inicios de sesión de System Manager mediante una clave FIDO2 (como YubiKey) como segunda forma de autenticación. De forma predeterminada, WebAuthn MFA está desactivado para los usuarios de ONTAP nuevos y existentes.

WebAuthn MFA es compatible con usuarios y grupos que utilizan los siguientes tipos de autenticación para el primer método de autenticación:

- Usuarios: Contraseña, dominio o nsswitch
- Grupos: Domain o nsswitch

Después de habilitar WebAuthn MFA como el segundo método de autenticación para un usuario, se solicita al usuario que registre un autenticador de hardware al iniciar sesión en System Manager. Después del registro, la clave privada se almacena en el autenticador y la clave pública se almacena en ONTAP.

ONTAP admite una credencial WebAuthn por usuario. Si un usuario pierde un autenticador y necesita reemplazarlo, el administrador de ONTAP debe eliminar la credencial WebAuthn del usuario para que el usuario pueda registrar un nuevo autenticador en el siguiente inicio de sesión.

> Los usuarios que tienen WebAuthn MFA habilitado como segundo método de autenticación necesitan usar el FQDN (por ejemplo, "https://myontap.example.com") en lugar de la dirección IP (por ejemplo, "https://192.168.100.200") para acceder a System Manager. Para los usuarios con MFA de WebAuthn habilitado, se rechazan los intentos de iniciar sesión en System Manager con la dirección IP.

Habilite WebAuthn MFA para los usuarios o grupos de ONTAP System Manager

Como administrador de ONTAP, puede habilitar WebAuthn MFA para un usuario o grupo de System Manager agregando un nuevo usuario o grupo con la opción MFA de WebAuthn habilitada o habilitando la opción para un usuario o grupo existente.

> Después de habilitar WebAuthn MFA como el segundo método de autenticación para un usuario o grupo, se solicitará al usuario (o a todos los usuarios de ese grupo) que registre un dispositivo de hardware FIDO2 en el siguiente inicio de sesión en System Manager. El sistema operativo local del usuario gestiona este registro y, por lo general, consiste en insertar la clave de seguridad, crear una clave de acceso y tocar la clave de seguridad (si es compatible).

Habilite WebAuthn MFA al crear un nuevo usuario o grupo

Puede crear un nuevo usuario o grupo con MFA de WebAuthn habilitado mediante System Manager o la CLI de ONTAP.

System Manager

1. Seleccione **Cluster > Settings**.
2. Seleccione el icono de flecha junto a **Usuarios y Roles**.
3. Seleccione **Agregar** en **Usuarios**.
4. Especifique un nombre de usuario o grupo y seleccione un rol en el menú desplegable para **Rol**.
5. Especifique un método de inicio de sesión y una contraseña para el usuario o el grupo.

   WebAuthn MFA soporta métodos de inicio de sesión de “contraseña”, “dominio” o “nsswitch” para los usuarios, y “dominio” o “nsswitch” para los grupos.

6. En la columna **MFA for HTTP**, selecciona **enabled**.
7. Seleccione **Guardar**.

CLI

1. Cree un nuevo usuario o grupo con WebAuthn MFA activado.

   En el siguiente ejemplo, WebAuthn MFA se habilita eligiendo “publickey” para el segundo método de autenticación:

```
security login create -user-or-group-name <user_or_group_name> \
                      -authentication-method domain \
                      -second-authentication-method publickey \
                      -application http \
                      -role admin
```

Habilite WebAuthn MFA para un usuario o grupo existente

Puede habilitar WebAuthn MFA para un usuario o grupo existente.

System Manager

1. Seleccione **Cluster > Settings**.
2. Seleccione el icono de flecha junto a **Usuarios y Roles**.
3. En la lista de usuarios y grupos, seleccione el menú de opciones para el usuario o grupo que desea editar.

   WebAuthn MFA soporta métodos de inicio de sesión de “contraseña”, “dominio” o “nsswitch” para los usuarios, y “dominio” o “nsswitch” para los grupos.
4. En la columna **MFA for HTTP** para ese usuario, seleccione **enabled**.
5. Seleccione **Guardar**.

CLI

1. Modifique un usuario o grupo existente para habilitar WebAuthn MFA para ese usuario o grupo.

   En el siguiente ejemplo, WebAuthn MFA se habilita eligiendo “publickey” para el segundo método de autenticación:

```
security login modify -user-or-group-name <user_or_group_name> \
                      -authentication-method domain \
                      -second-authentication-method publickey \
                      -application http \
                      -role admin
```

Leer más

Consulte las páginas del manual de ONTAP para obtener información sobre estos comandos:

- "seguridad de inicio de sesión creado"
- "modificación del inicio de sesión de seguridad"

Desactive WebAuthn MFA para usuarios de ONTAP System Manager

Como administrador de ONTAP, puede deshabilitar la MFA de WebAuthn para un usuario o grupo editando el usuario o grupo con System Manager o la interfaz de línea de comandos de ONTAP.

Desactive WebAuthn MFA para un usuario o grupo existente

Puede deshabilitar WebAuthn MFA para un usuario o grupo existente en cualquier momento.

> Si deshabilita las credenciales registradas, se conservan las credenciales. Si vuelve a activar las credenciales en el futuro, se utilizarán las mismas credenciales, por lo que el usuario no tendrá que volver a registrarse al iniciar sesión.

System Manager

1. Seleccione **Cluster > Settings**.
2. Seleccione el icono de flecha junto a **Usuarios y Roles**.
3. En la lista de usuarios y grupos, seleccione el usuario o grupo que desea editar.
4. En la columna **MFA for HTTP** para ese usuario, seleccione **Disabled**.
5. Seleccione **Guardar**.

CLI

1. Modifique un usuario o grupo existente para desactivar WebAuthn MFA para ese usuario o grupo.

   En el siguiente ejemplo, WebAuthn MFA se deshabilita seleccionando “none” para el segundo método de autenticación.

```
security login modify -user-or-group-name <user_or_group_name> \
                      -authentication-method domain \
                      -second-authentication-method none \
                      -application http \
                      -role admin
```

Leer más

Consulte las páginas del manual de ONTAP para este comando:

- "modificación del inicio de sesión de seguridad"

Vea la configuración MFA de ONTAP WebAuthn y administre las credenciales

Como administrador de ONTAP, puede ver la configuración MFA de WebAuthn para todo el clúster y administrar las credenciales de usuario y grupo para WebAuthn MFA.

Ver la configuración del clúster para WebAuthn MFA

La configuración del clúster de la MFA de WebAuthn se puede ver mediante la CLI de ONTAP.

Pasos

1. Vea la configuración del clúster para WebAuthn MFA. De manera opcional, puede especificar una máquina virtual de almacenamiento con `vserver` el argumento:

```
security webauthn show -vserver <storage_vm_name>
```

Ver los algoritmos MFA de clave pública soportados de WebAuthn

Es posible ver los algoritmos de clave pública compatibles con la MFA de WebAuthn para una máquina virtual de almacenamiento o para un clúster.

Pasos

1. Enumere los algoritmos MFA de WebAuthn de clave pública admitidos. De manera opcional, puede especificar una máquina virtual de almacenamiento con `vserver` el argumento:

```
security webauthn supported-algorithms show -vserver <storage_vm_name>
```

Vea las credenciales MFA registradas de WebAuthn

Como administrador de ONTAP, puede ver las credenciales de WebAuthn registradas para todos los usuarios. Los usuarios que no sean administradores que utilicen este procedimiento sólo pueden ver sus propias credenciales de WebAuthn registradas.

Pasos

1. Vea las credenciales MFA registradas de WebAuthn:

```
security webauthn credentials show
```

Quitar una credencial MFA de WebAuthn registrada

Puede quitar una credencial MFA de WebAuthn registrada. Esto es útil cuando la clave de hardware de un usuario se perdió, fue robada o ya no está en uso. También puede eliminar una credencial registrada cuando el usuario aún tiene el autenticador de hardware original, pero desea reemplazarla por una nueva. Después de eliminar la credencial, se le pedirá al usuario que registre el autenticador de reemplazo.

> Al quitar una credencial registrada para un usuario, no se deshabilita WebAuthn MFA para el usuario. Si un usuario pierde un autenticador de hardware y necesita iniciar sesión antes de reemplazarlo, debe eliminar la credencial mediante estos pasos y también "Desactive WebAuthn MFA" para el usuario.

System Manager

1. Seleccione **Cluster > Settings**.
2. Seleccione el icono de flecha junto a **Usuarios y Roles**.
3. En la lista de usuarios y grupos, seleccione el menú de opciones para el usuario o grupo cuyas credenciales desea eliminar.
4. Seleccione **Remove MFA for HTTP credentials**.
5. Seleccione **Quitar**.

CLI

1. Elimine las credenciales registradas. Tenga en cuenta lo siguiente:
   - Opcionalmente, puede especificar una máquina virtual de almacenamiento del usuario. Si se omite, la credencial se elimina en el nivel de clúster.
   - Opcionalmente, puede especificar un nombre de usuario del usuario para el que va a suprimir la credencial. Si se omite, la credencial se elimina del usuario actual.

```
security webauthn credentials delete -vserver <storage_vm_name>
-username <username>
```

Leer más

Consulte las páginas del manual de ONTAP para obtener información sobre estos comandos:

- "security webauthn show"
- "seguridad webauthn supported-algorithms show"
- "se muestran las credenciales de seguridad webauthn"
- "seguridad webauthn credenciales delete"

Información de copyright

Información de la marca comercial